Release Notes

FortiSOAR 7.6.6

March, 2026
FortiSOAR 7.6.6 Release Notes
00-400-000000-20210112

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-30	Initial release of 7.6.6

FortiSOAR 7.6.6 Release

Release 7.6.6 aligns with updated CA certificates from the FortiGuard Distribution Network (FDN) to ensure ongoing secure communication and stable license synchronization. Users on releases 7.6.5 or earlier are encouraged to upgrade to release 7.6.6 or later to get the updated CA certificates.

New Features and Enhancements

The FortiGuard Distribution Network (FDN) has updated its CA certificates. FortiSOAR release 7.6.6 includes the updated certificates to maintain secure communication with FDN services and prevent disruptions to license synchronization. Users on releases 7.6.5 or earlier are encouraged to upgrade to release 7.6.6 or later to get the updated CA certificates. This release does not include any additional features or enhancements.

Upgrade Information

You can upgrade your FortiSOAR enterprise instance, High Availability (HA) cluster, or a distributed multi-tenant configuration to release 7.6.6 using the following guidance.

> The FortiSOAR UI displays a notification when a new General Availability (GA) release is available. The notification includes a direct link to the release notes for more details.

Before You Upgrade

The upgrade process will temporarily take your FortiSOAR application offline. During this time, users will not be able to access or log in to the platform.

To ensure a smooth upgrade:

- **Notify users**: Inform all users in advance about the planned maintenance window and expected downtime.
- **Stop active processes**: Confirm that no critical playbooks, automations, or integrations are running before starting the upgrade.
- **Back up your system**: Perform backup of the FortiSOAR database and configuration to prevent data loss in case of unexpected issues.
- **Confirm prerequisites**: Verify that your environment meets all system requirements (OS version, disk space, dependencies, etc.).

Downgrading to previous firmware versions

Downgrading to previous firmware versions **is not supported**.

Upgrade Path

> ⚠ Releases 7.6.6 and later, and 7.5.3, include the updated CA certificates from the FortiGuard Distribution Network (FDN) to ensure secure communication and reliable license synchronization. If you upgrade to any other release, you must manually update the CA certificates on the FortiSOAR instance after the upgrade by following the steps in the Troubleshooting Tip: Action required: update FDN certificates for FortiSOAR instances article.

The following table provides version compatibility between FortiSOAR components and the supported upgrade paths:

Enterprise or MSSP Master Node	Supported Upgrade	Compatible Tenant Node	Compatible Agent	Compatible Secure Message Exchange (SME)
7.6.6 (c)	7.6.5-7.6.0 7.5.3 -7.5.0	7.6.5 -7.6.0 7.5.3 -7.5.0 **Important**: Since release 7.6.6 is mainly to get the updated CA certificates from the FortiGuard Distribution Network (FDN) to ensure ongoing secure communication and stable license synchronization, it is not necessary nor recommended to upgrade the external SME. **Note**: When upgrading to FortiSOAR 7.6.6 without upgrading the FortiSOAR Agents, users must also upgrade the Utilities Connector on the FortiSOAR Agent to ensure proper functionality.		
7.6.5 (c)	7.6.4-7.6.0 7.5.2 -7.5.0	7.6.4 -7.6.0 7.5.2 -7.5.0 **Note**: When upgrading to FortiSOAR 7.6.5 without upgrading the FortiSOAR Agents, users must also upgrade the Utilities Connector on the FortiSOAR Agent to ensure proper functionality.		
7.6.4 (c)	7.6.3-7.6.0 7.5.2-7.5.0	7.6.4 -7.6.0 7.5.2 -7.5.0 **Note**:Upgrade-only releases, such as 7.6.3 and 7.5.2, do not support upgrading external SMEs to these versions.		
7.6.3 (5) (c) (*upgrade-only release*)	7.6.2-7.5.0	7.6.3 -7.6.0, 7.5.2-7.5.0		7.6.2 -7.6.0, 7.5.1-7.5.0
7.6.2 (b) (c)	7.6.1-7.5.0	7.6.2-7.6.0		

7.6.1	7.6.0-7.5.0	7.6.1, 7.6.0	
7.6.0	7.5.2-7.5.0	7.6.0, 7.5.0	
7.5.3 (*upgrade-only release*)	7.5.2-7.5.0	7.5.3-7.5.0	
7.5.2 (5) (*upgrade-only release*)	7.5.0, 7.5.1	7.5.2-7.5.0	7.5.1, 7.5.0
7.5.1 (*upgrade-only release*)	7.5.0	7.5.1, 7.5.0, 7.4.5 -7.4.0	
7.5.0	7.4.5- 7.4.0	7.5.0, 7.4.5-7.4.0	
7.4.5 (4) (*upgrade-only release*)	7.4.4, 7.4.3	7.4.5-7.4.0	
7.4.4 (4) (*upgrade-only release*)	7.4.3-7.4.0	7.4.4-7.4.0	
7.4.3 (a) (4) (*upgrade-only release*)	7.4.2-7.4.0	7.4.3-7.4.0	
7.4.2 (4)	7.4.1, 7.4.0	7.4.2-7.4.0	
7.4.1 (3)	7.4.0	7.4.1, 7.4.0, 7.3.2	
7.4.0	7.3.3-7.3.0	7.4.0, 7.3.2	
7.3.3 (2) (*upgrade-only release*)	7.3.2, 7.3.1	7.3.3-7.3.1	
7.3.2 (2) (*upgrade-only release*)	7.3.1, 7.3.0	7.3.2-7.3.0	
7.3.1 (1)	7.3.0	7.3.1, 7.3.0	
7.3.0 (*for upgrade and migration support*)	7.2.2, 7.2.1	7.3.0	

Upgrade Notes:

- *Upgrade-only* releases contain critical usability and security enhancements. We advise users to upgrade their FortiSOAR setups to the latest releases corresponding to their installed FortiSOAR versions.
- (c) Upgrading from release 7.6.1 to a later release (for example, 7.6.4, 7.6.5 and later) causes the Utilities Connector '*Create an attachment from file*' action to fail. A workaround for this issue is described in the Known Issues and Workarounds chapter.
  Additionally, after upgrading from release 7.6.1, the TAXII server configuration is automatically disabled. If the TAXII server is required, manually re-enable it. For more information, see the Threat Intel Management Solution Pack documentation.
- (b) If you are upgrading your FortiSOAR HA cluster from releases 7.6.0, 7.5.2, 7.5.1, or 7.5.0 to release 7.6.1 or

later, follow the steps in the Upgrading to releases prior to 7.6.1 topic. If you are upgrading your FortiSOAR HA cluster from release 7.6.1 or later to release 7.6.2 or any subsequent release such as releases, 7.6.3, 7.6.4, 7.6.5, 7.6.6, you can use the 'rolling upgrades' process. Steps for rolling upgrade are mentioned in the Upgrading to releases post 7.6.1 topic.
The 'rolling upgrade' process, which minimizes downtime for high availability (HA) clusters, ***is not supported*** for Docker images.

- (**a**) Release 7.4.3 addresses a critical issue of connectors not working after backup and restore due to missing 'Python' dependencies, which affects fresh installations of FortiSOAR 7.4.2. Therefore, it is highly recommended to upgrade fresh installations of 7.4.2 instances to 7.4.3.

Compatibility Notes:

(**1**) No incompatibility issues were observed in MSSP use cases; however, the 'Manual Input' step operates differently in systems that have a lower-version tenant node and a higher-version master node since, FortiSOAR release 7.3.1 has an enhanced UI and upgraded functionality.

(**2**) No incompatibility issues were observed in MSSP use cases; however, in FortiSOAR release 7.3.1, the 'Complete' playbook environment can be passed to child playbooks, which was not possible in earlier versions, leading to some differences in systems that have a lower-version tenant node and a higher-version master node.

(**3**) Pushing approval playbooks from FortiSOAR release 7.4.1 master node to a lower-version tenant node is not supported. In such cases, the playbook is not visible on the tenant node, and neither will FortiSOAR display any error.

(**4**) No incompatibility issues were observed between versions 7.4.2, 7.4.3, and 7.4.4 of the FortiSOAR enterprise/MSSP-master and FSR agent, Secure Message Exchange (SME), or MSSP-tenants.
However, it is important to consider the following when using versions 7.4.2, 7.4.3, or 7.4.4 of the FortiSOAR enterprise/MSSP-master with 7.4.0 or 7.4.1 versions of FSR agent or MSSP-tenants:
In the case of MSSP environments, it is recommended that you upgrade both the master and tenant nodes to release 7.4.4 or 7.4.3. If your master and tenant nodes are both not upgraded to release 7.4.4 or 7.4.3, take note of the following:

- Ensure that you synchronize records along with their relationships when you use the 'Sync Records' feature, if your master node is on release 7.4.2 or later, and your tenant nodes are on release earlier than 7.4.2, such as 7.4.1 or 7.4.0.
- To download 'FSR Agent/Tenant node' logs, both the master and agent/tenant must be on release 7.4.2 or later. If the master node is on release 7.4.2 or later, and the agent is on a release earlier than 7.4.2, the log download is unsuccessful and returns an error such as "`For agents, log collection is accessible on version 7.4.2 and beyond`".
- Replication from a tenant node that is on release 7.4.1 or 7.4.0 to a master node that is on release 7.4.2 or later will not fail if related records are not present on the master node. However, in the same case, replication from the master node to tenant nodes will fail if related records are not present on the tenant node.
- The update record request fails when the record is unavailable at the replicated end when a tenant node is on release 7.4.1 or 7.4.0, and the master node is on release 7.4.2 or later.

(**5**) Releases 7.5.2 and 7.6.3 are upgrade-only releases and upgrading an external FortiSOAR SME to both these releases are not supported.

Upgrade Procedure

> During the upgrade, you are prompted to reset and confirm the root password. If the entries match, the password is updated. If they do not match, the prompt is shown again. Entering n skips this step and continues the upgrade without resetting the password. You have up to three attempts to enter matching passwords; if all attempts fail, the upgrade is marked as failed.
> Review and respond to all upgrade prompts carefully. If the root password reset is skipped, it must be reset later from the VM console. Refer to the Red Hat or Rocky Linux documentation for instructions.

> After login, the csadm user has limited sudo privileges. For security reasons, root access is available only via the system console and not over SSH.

The upgrade process for FortiSOAR enterprise systems is as follows:

1. Connect to the FortiSOAR VM via SSH and start a `tmux` session.
2. Run the following command to check if your system is ready for an upgrade to release 7.6.6 :
   ```
   sudo csadm upgrade check-readiness --target-version 7.6.6
   ```
3. (Optional) Resolve any validation failures and rerun the check to confirm readiness.
   Important: Run the readiness check before upgrading to ensure success.
4. Run the following command to upgrade your system to release 7.6.6:
   ```
   sudo csadm upgrade execute --target-version 7.6.6
   ```
   Note: The system’s appliance host key changes during the upgrade.

For detailed procedures, including preparation steps and instructions for High Availability setups, multi-tenancy environments, and Docker deployments, see the Upgrade Guide.

After the Upgrade

Once the upgrade is complete, perform these checks to ensure system stability and optimal performance:

- **Clear browser cache**: Clear your cache and log out before signing back in to avoid any UI or functionality issues.
- **Verify key functions**: Review key system areas such as playbook audit logs, user access, and automation services.
- **Validate integrations**: Confirm that all connectors, integrations, and scheduled jobs are working properly.
- **Monitor performance**: Observe system health metrics and logs for any irregular behavior in the hours following the upgrade.

Product Integration and Support

Web Browsers & Recommended Resolution

FortiSOAR 7.6.6 User Interface has been tested on the following browsers:

- Google Chrome version 146.0.7680.165
- Mozilla Firefox version 149.0
- Microsoft Edge version 146.0.3856.72
- Safari version 26.1 (20622.2.11.119.1)
- The recommended minimum screen resolution for the FortiSOAR GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI might not get properly displayed.

Virtualization

This section lists FortiSOAR version 7.6.6 product integration and support for virtualization:

- AWS Cloud
- Fortinet-FortiCloud
- VMware ESXi versions 5.5, 6.0, 6.5, 7.0, and 8.0
- Redhat KVM

> For any other virtualization or cloud hosting environment, such as GCP, Azure, OCI, or OCI DRCC, you can install Rocky Linux 9.3/9.4/9.5/9.6 or RHEL 9.3/9.4/9.5/9.6 and then install FortiSOAR using the FortiSOAR CLI installer. Note that release 7.6.6 has been tested with RHEL 9.6 and Rocky Linux 9.6. For more information, see the "Deployment Guide."

Resolved Issues

FortiSOAR release 7.6.6 aligns with updated CA certificates from the FortiGuard Distribution Network (FDN) to ensure continued secure communication and stable license synchronization. This release does not include any additional bug fixes or enhancements.

Known Issues and Workarounds

- **1126843**: When a filter is applied on the listing page and a record is opened in a new tab, users may encounter a '`414 Request-URI Too Large`' error if the URL generated with the filters exceeds the default length limits.
  Workaround:
  To resolve this issue, increase the buffer size for client headers in your **Nginx** configuration file.
  Update the `large_client_header_buffers` setting from `4 8k;` to `4 50k;` in the `/etc/nginx/nginx.conf` file.
  After making the change, restart the '`nginx`' service as the '`root`' user to apply the changes by running the following command:
  ```
  # systemctl restart nginx
  ```
  If you are using HAProxy as a load balancer, follow these steps:
  a. SSH to your HAProxy VM and log in as *root* user.
  b. Edit `/etc/haproxy/haproxy.cfg` file.
  c. In the '`global`' section, add the following parameter:
  ```
  tune.bufsize 32768
  ```
  d. Restart HAProxy to apply the changes by running the following command:
  ```
  # systemctl restart nginx
  ```
- **1132542**: After upgrading a FortiSOAR deployment configured with Multi-Tenancy (MSSP) and High Availability (HA) in an Active-Active cluster, the WebSocket connection on the secondary node remains disconnected.
  Workaround:
  Restart the `cyops-tomcat` service on the secondary node:
  ```
  #systemctl restart cyops-tomcat
  ```
  This restores the WebSocket connection on the secondary node and ensures that all nodes are properly connected.
- **1220684**: Upgrading from release 7.6.1 to a later release (for example, 7.6.4, 7.6.5) causes the Utilities Connector '*Create an attachment from file action*' to fail with the following error:
  ```
  CS-INTEGRATION-5: Error occurred while executing the connector action. ERROR :: 400 Client
  Error: Bad Request for url: https://localhost/api/3/files :: {'type': 'TypeError',
  'message': \"Internal Server Error. Check log 'prod.log' for more details\"} :: Url:
  https://localhost/api/3/files Call for URL: https://localhost:9595/integration/execute/
  failed with status code 400 \n
  ```
  The issue occurs because the **Restricted File MIME Types** setting under **Settings** > **Application Configuration** has no values configured. As a result, file uploads fail.
  Workaround:
  After upgrading from release 7.6.1:
  a. Navigate to **Settings** > **Application Configuration**.
  b. Update **Restricted File MIME Types** to include the default values:
  ```
  image/svg
  image/svg+xml
  ```
  c. If any custom MIME types were configured before upgrading from release 7.6.1, re-add those values as well.
  d. Save the updated settings.
  For details, see the Enabling MIME type validations for file uploads topic in the "Administration Guide."
  NOTE: After upgrading from release 7.6.1, the TAXII server configuration is also automatically disabled. If the TAXII server is required, manually re-enable it. For more information, see the Threat Intel Management Solution Pack documentation.

www.fortinet.com